REMARKS

Applicants respectfully request further examination and reconsideration in view of the instant response. Claims 1-34 remain pending in the case. Claims 1-34 are rejected. Claims 1-6, 13-17, 22, 23, 27, 29, 31 and 32 are amended herein. No new matter has been added as a result of the claim amendments. Support for the amendments can be found in the instant specification at least at page 16, line 1, through page 23, line 17, and corresponding Figures 4A, 4B, 5A and 5C.

103(a) Rejections - Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34

The instant Office Actions states that Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over "Secure Scalable Video Streaming for Wireless Networks" by Wee et al., hereinafter referred to as "Wee," in view of U.S. Patent No. 5,790,669 by Miller et al., hereinafter referred to as "Miller." The Applicants have reviewed Wee and Miller and respectfully submit that the present invention as recited in Claims 1, 2, 5-10, 12, 13, 23-30 and 32-34 are patentable over the combination of Wee and Miller, for at least the following rationale.

Applicants respectfully direct the Examiner to independent Claim 1 that recites that an embodiment of the present invention is directed to (emphasis added):

> A method for ensuring the integrity of data, comprising:
> a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums,

wherein said plurality of first data segments have a different priority than said plurality of second data segments; and

enabling said cryptographic checksums for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

Independent Claims 23, 27, 29 and 32 include similar recitations. Claims 2, 5-10, 12 and 13 that depend from independent Claim 1, Claims 24-26 that depend from independent Claim 23, Claim 28 that depends from independent Claim 27, Claim 30 that depends from independent Claim 29, and Claims 33 and 34 that depend from independent Claim 32 also include these recitations.

"As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)). Applicants note that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

Moreover, Applicants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.02(VI); *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)).

Applicants note that the instant Office Action recites that "Wee does not disclose calculating a cryptographic checksum for said plurality of first data segments" (Office Action mailed January 30, 2008; page 4, lines 6-7). Therefore, Applicants respectfully submit that Wee does not disclose "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" as recited in independent Claim 1, and similar recitations of independent Claims 23, 27, 29 and 32. Applicants understand the instant Office Action to rely on Miller as overcoming this deficiency.

First, Applicants respectfully submit that Miller also does not teach, describe or suggest "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" as recited in independent Claim 1, and similar recitations of independent Claims 23, 27, 29 and 32.

As understood by the Applicants, Miller discloses a non-repudiation system in which the contents of messages are verified using a cryptographic

hash function (col. 2, lines 18-57). Miller recites that "[r]eliability in the Netscape SSL protocol is provided by a common hash function that is applied by a sender to the contents of each outgoing packet and by a receiver to the contents of each incoming packet" (emphasis added; col. 1, lines 28-31). Moreover, in a second embodiment, Miller recites

> The hash values computed by the first entity include a first outgoing hash value that represents the accumulated total of the hash function applied to each of the messages in the first stream since the start position and a first incoming hash value that represents the accumulated total of the hash function applied to each of the messages in the second stream received by the first entity since said start position. The hash values computed by the second entity include a second outgoing hash value representing the accumulated total of the hash function applied to each of the messages in the second stream since the start position and a second incoming hash value representing the accumulated total of the hash function applied to each of the messages in the first stream received by the second entity since the start position. (emphasis added)

Accordingly, Applicants understand Miller to disclose computing hash values for entire messages, and accumulating these hash values.

Therefore, Applicants respectfully submit that Miller does not teach, describe or suggest "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" (emphasis added) as claimed. Moreover, by disclosing that a hash value is computed for an entire message, Applicants respectfully submit that Miller teaches away from the claimed embodiments.

Second, Applicants respectfully submit that Miller does not disclose that to which it is asserted as teaching. Specifically, the instant Office Action recites that "Miller discloses calculating a cryptographic checksum for said plurality of data segments (col. 1 lines 27-44)" (emphasis added; Office Action mailed January 30, 2008; page 4, lines 9-10). In contrast, Miller specifically recites "[o]ther prior art systems provide similar reliability checks by applying the well-known parity, checksum and CRC (cyclic redundancy checking) functions to the outgoing and incoming messages" (emphasis added; col. 1, lines 38-41). Moreover, Miller goes on to recite "[w]hile the Netscape SSL provides secure and reliable network communications, it and many other prior art network security systems do not provide a general property of non-repudiation" (emphasis added; col. 1, lines 41-45).

In particular, Applicants understand Miller to disclose the use of a non-cryptographic checksum, in that the recited checksum does not provide for non-repudiation. Therefore, Applicants respectfully submit that Miller does not disclose a cryptographic checksum as claimed.

Third, Applicants respectfully assert that the relied upon disclosures of Miller, (1) the non-cryptographic checksum recited in the Background of the Invention section (col. 1, lines 28-45) and (2) the cryptographic hash of the described invention (at least col. 2, line 35, through col. 3, line 33), are mutually exclusive, and that there is no teaching or suggestion to modify either of the disclosures in the manner suggested in the Office Action.

As presented above, Applicants understand Miller to disclose the use of a non-cryptographic checksum, in that the recited checksum does not provide for non-repudiation. In contrast, the described invention of Miller describes the use of a cryptographic hash function. Applicants respectfully submit that by explicitly disclosing the shortcoming of prior art systems including checksums as not providing non-repudiation, and by disclosing the cryptographic hash function as overcoming this shortcoming, that there is no teaching, suggestion or motivation within Miller to modify either of the different disclosures in the manner suggested in the current Office Action, and that these disclosures are mutually exclusive.

Applicants respectfully assert that the combination of Wee and Miller does not teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 23, 27, 29 and 32, that this claim overcomes the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Therefore, Applicants respectfully submit that the combination of Wee and Miller also does not teach or suggest the additional claimed features of the present invention as recited in Claims 2, 5-10, 12 and 13 that depend from independent Claim 1, Claims 24-26 that depend from independent Claim 23, Claim 28 that depends from independent Claim 27, Claim 30 that depends from independent Claim 29, and Claims 33 and 34 that depend from independent Claim 32. Therefore, Applicants respectfully submit that Claims 2, 5-10, 12, 13, 24-26, 28, 30, 33 and 34 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

103(a) Rejections - Claims 3, 4, 11, 14-22 and 31

The instant Office Actions states that Claims 3, 4, 11, 14-22 and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wee in view of Miller, further in view of U.S. Patent Application Publication No. 2002/0095586 by Doyle et al., hereinafter referred to as the Doyle reference. The Applicants have reviewed Wee, Miller and Doyle and respectfully submit that the present invention as recited in Claims 3, 4, 11, 14-22 and 31 are patentable over the combination of Wee, Miller and Doyle, for at least the following rationale.

Claims 3, 4 and 11 are dependent on independent Claim 1 and include the recitations of Claim 1 and Claim 31 is dependent on independent Claim 29. Hence, by demonstrating that Wee, Miller and Doyle do not show or suggest the limitations of independent Claims 1 and 29, it is also demonstrated that Wee, Miller and Doyle do not show or suggest the embodiments of Claims, 3, 4, 11 and 31.

As presented above, Applicants respectfully submit that the combination of Wee and Miller does not teach, describe or suggest the recitations of independent Claims 1 and 29. Furthermore, Applicants respectfully submit that the combination of Wee and Miller does not teach, describe or suggest the similar recitations of independent Claim 14.

Applicants respectfully submit that Doyle does not overcome the shortcomings of the combination of Wee and Miller. As understood by the Applicants, Doyle discloses a technique for continuous user authentication. In

particular, Applicants respectfully submit that Doyle also does not teach, describe or suggest "calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums" as claimed. In particular, Applicants respectfully submit that Doyle is silent to such a teaching.

Therefore, Applicants respectfully submit that Doyle shares at least some of the shortcomings of Wee and Miller. Thus, Doyle, alone or in combination with Wee and/or Miller, does not show or suggest the embodiments as claimed.

Applicants respectfully assert that the combination of Wee, Miller and Doyle does not teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 14 and 29, that this claim overcomes the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Therefore, Applicants respectfully submit that the combination of Wee, Miller and Doyle also does not teach or suggest the additional claimed features of the present invention as recited in Claims 3, 4 and 11 that depend from independent Claim 1, Claims 15-22 that depend from independent Claim 14, and Claim 31 that depends from independent Claim 29. Therefore, Applicants respectfully submit that Claims 3, 4, 11, 15-22 and 31 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

CONCLUSION

In light of the above remarks, Applicants respectfully request reconsideration of the rejected claims. Based on the arguments presented above, Applicants respectfully assert that Claims 1-34 overcome the rejections of record, and therefore Applicants respectfully solicit allowance of these claims.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER BLECHER LLP

Date: April 28, 2008

/John P. Wagner, Jr.

John P. Wagner, Jr.
Reg. No. 35,398

Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076

(408) 377-0500
Facsimile: (831) 763-2895